Dosya Entegrasyonu Etki Alanında Anomali Tespiti İçin Bir Ontoloji Geliştirimi

Araştırma Makalesi/Research Article

Özgü CAN*, Murat Osman ÜNALIR, İbrahim ÜZÜM

Bilgisayar Mühendisliği Bölümü, Ege Üniversitesi, İzmir, Türkiye
ozgu.can@ege.edu.tr, murat.osman.unalir@ege.edu.tr, ibrahim.uzum@windowslive.com
(Geliş/Received:25.11.2018; Kabul/Accepted:25.07.2019)
DOI: 10.17671/gazibtd.487373

***Özet*—** Günümüzde, veri depolama ve yazılım geliştirme teknolojilerinin çeşitliliğinde büyük bir artış yaşanmıştır. Hızla gelişen ve değişen teknolojiler sebebiyle, ortak çalışan organizasyonlardaki entegrasyon ve çok çeşitlilik, temel bir sorun olarak ortaya çıkmaktadır. Bu kapsamda dosya entegrasyonları, farklı iş platformları arasındaki veri bütünleştirmesine yardımcı olan etkili bir çözüm olarak sunulmaktadır. Böylelikle, farklı elektronik sistemler arasındaki rutin iş süreçleri ve iş mantıkları otomatize edilebilmektedir. Anomali tespiti, sistemlerde meydana gelebilecek anormal durumları tespit eden bir veri analiz işlemidir. Anomali tespiti, bilgi tabanlı sistemlerde beklenmedik durumlara karşı farkındalık ve beklenen davranışa uymayan anomaliler karşısında gerekli eylemlerin yerine getirilmesini sağlamaktadır. Bu nedenle, anomali tespiti dosya entegrasyonlarında meydana gelen anomalilerin tespiti için önemli bir veri analizi işlemidir. Bu çalışma kapsamında, dosya entegrasyonu sistemlerinde gerçekleşen anomalileri tespit edebilmek için ontoloji tabanlı bir yaklaşım sunulmaktadır. Dosya entegrasyonlarında anormalliklerin tespiti, bilgi güvenliği üçlüsünden (gizlilik, bütünlük ve kullanılabilirlik) biri olan kullanılabilirlik açısından önemlidir. Entegrasyonlardaki anomalilerin büyük bir kısmı veri bütünlüğüne yöneliktir ve bu anomaliler transfer süresinden ya da gelen dosya boyutundan tespit edilerek yakalanabilmektedir. Önerilen ontolojik yaklaşımda, örnek bir sisteme yapılan dosya entegrasyonları sorgulanarak entegrasyon işlemlerinde meydana gelen anomaliler tespit edilebilmektedir. Önerilen yaklaşımın, dosya entegrasyon sistemlerinde veri bütünlüğüne ve kullanılabilirliğe (dosya akışını durdurabilecek anomaliler) yönelik anormal durumlara karşı ontoloji bazlı bir çözüm sunması amaçlanmaktadır.

***Anahtar Kelimeler*—** anlamsal web, ontoloji, bilgi temsili, veri güvenliği, anomali tespiti, bilgi sistemleri

An Ontology Development for Anomaly Detection in File Integration Domain

***Abstract*—** Nowadays, there has been an enormous increase in the variety of data storage and software development technologies. Integration and diversity in collaborative organizations emerge as a fundamental problem due to the rapidly evolving and changing technologies. In this context, file integration comes out as an effective solution in order to integrate data between different business platforms. Thus, routine business processes and business logic of different electronic systems could be automated. Anomaly detection is a data analysis process that detects abnormal situations in systems. Anomaly detection provides an awareness for the unexpected situations in information based systems and the fulfillment of necessary actions against anomalies that do not comply with the expected behavior. Therefore, anomaly detection is an important data analysis process to detect anomalies that occur in file integrations. In this study, an ontology based approach is presented in order to detect anomalies in file integration systems. Anomaly detection in file integrations is important in terms of availability which is one of the component of information security triad (confidentiality, integrity, availability). Most of the anomalies in integrations are oriented to data integrity and these anomalies can be detected from the transfer time or the incoming file size. In the proposed ontological approach, the file integrations made to a sample system are being queried and anomalies that occur in the integration processes are being detected. The proposed approach is intended to provide an ontology-based solution to data integrity and availability (anomalies that can stop the file flow) in the file integration systems.

***Keywords*—** semantic web, ontology, knowledge representation, data security, anomaly detection, information systems

1. GİRİŞ (INTRODUCTION)

İş süreçlerinin elektronikleşmesi ve otomatize edilmesi ile birlikte, son yıllarda çeşitli sayıda yazılım geliştirme ve veri depolama teknolojisi ortaya çıkmıştır. Sürekli artış gösteren bu çeşitlilik, farklı iş platformları arasındaki teknoloji tutarlılıklarının sağlanamaması gibi sorunları da beraberinde getirmiştir. Bu sebeple, farklı teknolojilere sahip sistemler arasında bir köprü görevi görecek ara katman yazılımlarına ihtiyaç doğmuştur. Bu kapsamda dosya entegrasyonları, değişik teknolojilere sahip sistemler arasında standartlara dayalı veri alışverişleri ve veri bütünleştirmelerine yardımcı olmaktadır. Dosya entegrasyonu sistemleri, dağıtık sistemler arasında belirli standartları temel alarak dosya transferi işlemi aracılığıyla veri ve iş süreci otomasyonu gerçekleştiren sistemlerdir. Dosya entegrasyonları sayesinde; platform farklılıkları, veri tutarsızlıkları ve ortak sistemler arasındaki iletişim sorunları en aza indirgenmektedir. Bunun sonucunda, ortak sistemler birbirleri arasında ortak iş akışları yaratma olanağı elde etmektedir. Böylelikle, farklı kurumlar ya da bir kurumun dağıtık yapıdaki alt kuruluşları arasında gerçekleşen veri alışverişinin standartlara dayalı bir yapıda gerçekleşmesi sağlanmaktadır.

Bilgi sistemlerinin iş süreçlerini ve iş mantığını yönetebilmesini sağlayan dosya entegrasyonu sistemleri dijital dönüşümün önemli bir parçasıdır. Dosya entegrasyonları, ayrık sistemler arasındaki veri bütünleştirmelerinde en yaygın olarak kullanılan yöntemlerden biridir. Entegrasyonlar sayesinde, bilgi sistemlerinde ortak veri yapılarına dayanan iletişim altyapıları oluşturulmaktadır. Dosya entegrasyonları, iki ortak sistem arasındaki verileri senkronize edecek ve bu sistemlerdeki iş akışlarını karşılıklı olarak yönetebilecek bir ortam sağlamaktadır. Elektronik fatura, döviz kuru ya da hava durumu akışları gibi sektöre dayalı örnekler, dosya entegrasyonlarının en popüler kullanım alanları olarak gösterilmektedir. Verilen örneklere bakılarak, dosya entegrasyonlarının elektronik sistemler için kritikliği anlaşılabilmektedir. Tüm bu etkenlerden dolayı, dosya entegrasyon sistemleri günümüzde kurumların en önemli bilgi sistemi yapıtaşlarından biridir.

Anomali tespiti, bir işlem ile ilgili olarak anormal ya da beklenmedik durumların tespiti için ilgili örüntülerin bulunması işlemidir. Chandola vd. [1] tarafından yapılan tanımda, anomali tespiti, beklenen davranışa uymayan verilerdeki örüntüleri bulma problemi olarak ifade edilmekte ve bu uyumlu olmayan örüntülere anomali denmektedir. Çok sayıda farklı uygulama etki alanında (*domain*) anomalilerle karşılaşılabilmektedir. Örneğin, bilgisayar ağlarına yönelik saldırı tespit sistemlerinde [2], finans alanında [3] ve klinik etki alanında [4] anomalilerin tespitlerine yönelik çalışmalar yapılmaktadır. Bu uygulama etki alanlarına ek olarak, dosya entegrasyon sistemlerinde de anomali tespiti yapılmalıdır. Bu kapsamda, dosya entegrasyonlarında meydana gelebilecek gerçek zamanlı anomalilerin tespit edilmesi, ilgili kişilerin uyarılması ve bu kapsamdaki raporlamanın gerçekleştirilmesi gerekmektedir. Dosya entegrasyonu sistemleri için anomali tespiti: (i) transferi gerçekleşen dosyalarda boyut ve entegrasyon süresi kapsamında anomalilerin zamanında fark edilmesini, (ii) dosya içeriğinin kontrol edilmesini ve müdahalenin yapılmasını, (iii) dosyada veri bütünlüğü kapsamında meydana gelen ihlallerin engellenebilmesini, (iv) anormalliklerin izlenebilirliğini (v) entegrasyon kanallarının sürekliliğini ve kullanılabilirliğini sağlayabilmektedir.

Entegrasyon temelli çalışan sistemlerde günlük transfer edilen dosya sayısı ortalama olarak yarım milyon adedi bulabilmektedir. Bu olağan akış, sistem ağına ve entegrasyon kanallarına belirli bir yük getirmektedir. Özellikle dosya boyutları ve dosya transfer zamanındaki anormallikler, bant genişliği yükünü artırıp entegrasyon kanallarının kullanılamaz hale gelmesine sebep olmakta, dolayısıyla dosya transferi gecikmeleri yaşanmaktadır. Bu durum, bilgi güvenliğinin temel ilkelerinden biri olan ağın kullanılabilirliğini tehdit etmektedir. Tespit edilen anormal dosyalardaki sorunlar genellikle veri bütünlüğüne yönelik durumlar olup; bozuk içerikli XML (*eXtensible Markup Language*) [5], varlık genişletme, zorlayıcı ayrıştırma (*coersive parsing*), içerik değiştirme ve sunucu taraflı sahtecilik istekleri gibi örnekler şeklinde görülebilmektedir [6]. Dosya entegrasyonlarında veri bütünlüğüne yönelik bu durumlar, yüksek oranda dosya boyutu ya da entegrasyon süresi anomalileri olarak tespit edilmektedir.

Dosya entegrasyonlarında anomali tespitine yönelik bir çözüm geliştiriminde teknoloji ya da spesifik veritabanı bağımlı bir yönteme başvurulması, standartlara dayanan bir yapı oluşturulması açısından yeterli değildir. Birçok dosya entegrasyon teknolojisi ve dağıtık bilgi sistemleri bazında değişik yapılarda veritabanları bulunmaktadır. Geliştirilecek anomali tespit sisteminde, teknoloji bağımsız olmak ve ortaya bir bilgi temeli sunmak kritiktir. Bu doğrultuda; bu çalışmada, genelleştirilmiş, genişletilebilir, standart temelli ve yeniden kullanılabilir bir yapı ortaya koymak amacıyla Anlamsal Web temelli ontoloji tabanlı bir çözüm sunulmaktadır. Böylelikle, dosya entegrasyonu kapsamında varlık modellemesine dayalı bir ontoloji geliştirilmesi ve mevcut bilgi güvenliği tabanlı anomali tespitine yönelik ontolojilere katkı sunmak amaçlanmaktadır. Dosya entegrasyonlarında anlamsal ifade edilebilirlik sağlanacak ve dosya entegrasyonu etki alanında bir bilgi tabanı oluşturulacaktır.

Bu çalışmanın organizasyonu şu şekildedir: ikinci bölümde çalışmanın hedefi anlatılmakta, üçüncü bölümde literatür araştırması sunulmakta, dördüncü bölümde anomali tespiti için geliştirilen ontoloji açıklanmaktadır. Beşinci bölümde ontolojik çalışmanın bir değerlendirmesi sunulmakta, altıncı bölümde ise sonuçlar ve gelecek çalışmalar özetlenmektedir.

2. HEDEF (GOAL)

Dosya entegrasyonları, sistemler arası hassas bilgi akışını yönetmesi sebebiyle güvenlik düzeyi yüksek bir etki alanıdır. Özellikle dosya boyutu ve entegrasyon işlem

süresi bazındaki anomalilerin tespiti, sistemler arasındaki veri kaybının önlenmesi açısından kritiktir. Anomali tespitinde ontolojik bir çözüm yaklaşımı sunulması, değişik teknolojiler kullanan sistemlere yönelik, operasyon bağımsız ve standart temelli bir yapı oluşturulmasını sağlayacaktır. Ontolojik model ile, dosya entegrasyon etki alanında platform özelleştirmesi ya da veri entegrasyonu yapmaya gerek kalmadan anormal bulguların tespiti sağlanabilecektir.

İlgili çalışmada dosya entegrasyonu tabanlı bilgi sistemleri için ontolojik bir anomali tespit çözümü sunulmaktadır. Belirtilen bu ontoloji tabanlı yaklaşım, [7, 8] çalışmalarında önerilen bilgi güvenliğinin sağlanmasını hedefleyen dosya entegrasyonlarına yönelik anomali tespit sistemini temel almaktadır. Bu çalışmada önerilen ontoloji tabanlı yaklaşımda amaç, dosya entegrasyonu temelli çalışan sistemlerde gelen dosyaların boyutları ve entegrasyon süreleri kapsamında anomalileri belirleyecek bir ontoloji geliştirmektir. Önerilen bu çalışma ile entegrasyonlardaki anormal durumlara farkındalık ve müdahale imkânı sağlayan bir anlamsal çözüm önerisi sunulmaktadır. Sonuç olarak bu çalışmada, dosya entegrasyonları etki alanında anomali tespitine yönelik kural tabanlı ontolojik bir çözüm hedeflenmektedir.

3. LİTERATÜR ÇALIŞMASI (LITERATURE STUDY)

Literatürde yer alan çalışmalar incelendiğinde, farklı uygulama alanlarında ontoloji tabanlı yaklaşımın kullanıldığı [9, 10, 11], anomali tespitine yönelik ontoloji tabanlı yaklaşımların ise ağ saldırı tespitleri, işletim sistemleri, web uygulamaları, akıllı ev sistemleri, iş süreci yönetim sistemleri ve metin içerikleri gibi belirli uygulama alanlarında yoğunlaştığı görülmektedir.

Ağ saldırı tespitleri kapsamında, Abdoli ve Kahani [12], ontoloji tabanlı dağıtık bir saldırı tespit sistemine (*intrusion detection system* - IDS) yönelik bir çalışma sunmaktadır. İlgili çalışmada, IDS amacıyla bilgisayar saldırıları taksonomisi kullanılarak bir atak ontolojisi geliştirilmiştir. Anlamsal Web'in saldırı tespit sistemlerinde kullanılabilirliği incelenmiş, ataklar genel olarak; virüs, solucan, aşırı yükleme, hizmetin reddi (*denial of service* - DoS), ağ, parola ve truva atı saldırıları olmak üzere yedi ana sınıfa ayrılmıştır.

Hsieh ve diğerlerinin sunduğu çalışmada ise [13], kablosuz sensor ağları (*wireless sensor networks* - WSN) için ontoloji tabanlı bir saldırı tespit sistemi önerilmektedir. Çalışmada, bir saldırı tespit bilgi tabanı oluşturularak WSN tabanlı iletişim sistemlerindeki anomalilerin tespit edilmesi hedeflenmektedir. Ontoloji tabanlı saldırı tespit sistemlerine yönelik bir diğer çalışma Hung ve Liu [14] tarafından sunulmuştur. İlgili çalışmada, ağ saldırı tespitleri etki alanındaki mevcut terimler bazında temel bir varlık ve ilişki kümesi oluşturulmaktadır. Bu temel yapı kullanılarak, dış kullanıcıların ve etki alanı uzmanlarının belirtimleri bazında ontolojinin özelleştirilmesini sağlayan bir yapı oluşturulmaktadır. Böylelikle, saldırı tespitlerinde ontolojilerdeki çıkarsama özelliği kullanılarak daha akıllı bir tespit sisteminin geliştirilebileceği savunulmaktadır.

Can vd. çalışmasında [15], işletim sistemlerindeki kötücül yazılım niteliğindeki saldırıları tarayan ve tespit eden ontolojik bir yaklaşım sunulmaktadır. İlgili çalışmada ontolojiler kullanılarak saldırı tespit sistemleri bazında anlamsal bir ifade ve bilgi tabanı yaratmak amaçlanmaktadır. Bir IDS ontolojisi yaratılarak, işletim sistemindeki hareketler incelenmekte ve bulgular önceden tanımlanmış bir kötücül yazılım veritabanındaki kayıtlar ile karşılaştırılmaktadır. Önerilen sistem ile, mevcut kötücül yazılım taramalarının zaman maliyetinin düşürülmesi ve saldırı tespitinin performansının artırılması hedeflenmektedir.

Kolaczek vd. çalışmasında [16], ağ trafiğindeki anomalilerin tespiti amacıyla ontoloji tabanlı bir atak tanıma sistemi önerilmektedir. İlgili çalışmada, etki alanı uzmanlığının daha kolay üretilmesi amacıyla bir saldırı tespit uygulaması tasarlamak ve geliştirmek için yeni bir yaklaşım sunulmaktadır. Çalışmada, trafik anomalileri tespitinin rolü ortaya konmakta, ağ iletişimini karakterize eden bazı özel değerlerin, güvenlik olaylarının (solucan saldırısı, virüs yayılması) neden olduğu ağ anormalliklerini tespit etmek için nasıl kullanılabileceği tartışılmaktadır.

Karande ve Gupta tarafından sunulan çalışmada [17], web uygulaması güvenliği için ontoloji tabanlı bir saldırı tespit sistemi geliştirilmiştir. Önerilen sistemde bağlantılar ve betiklerden gelen bilgilerin takibi ve olası saldırıların tespit edilmesi hedeflenmektedir. Önerilen ontoloji tabanlı IDS modeli, protokollere özel saldırıları algılamakta ve kötü amaçlı betikleri tanımlamaktadır.

Anomali tespitlerine yönelik ontolojik çalışmalar, akıllı ev gibi otomasyon temelli sistemleri de çalışma alanı olarak kullanabilmektedir. Pardo vd. çalışmasında [18], akıllı ev sistemlerinde gerçekleşen günlük yaşam aktivitelerindeki anomalilerin tespitine yönelik ontoloji tabanlı bir çerçeve önerilmektedir. Çalışm, bağlamsal bir veritabanı sayesinde akıllı ev asistan sistemlerinin günlük yaşam aktivitelerini çıkarsamakta ve böylece evde meydana gelen anormal davranışları tespit edebilmektedir. Bu kapsamda, akıllı ev sistemleri gibi heterojen ortamlarda kullanılabilen bir ontoloji tabanlı anomali tespit yöntemi sunulmaktadır. Bu çalışmada ontoloji, ev içerisindeki cihazlar arasında birlikte çalışılabilirliği sağlamak için kullanılmaktadır.

Literatürde, ontolojik çalışmaların güvenlik bazlı hatalı konfigürasyonların anomali olarak tespitinde rol aldığı görülmektedir. Raad vd. tarafından sunulan çalışmada [19], Anlamsal Web kullanılarak web üzerindeki hatalı kimlik bağlantılarını anomali olarak tespit eden bir sistem ortaya konulmaktadır. Çalışmada, farklı ontolojilerdeki farklı isimlerin aynı varlığı işaret edebildiği ve "owl:sameAs" niteliğinin yanlış kullanılabildiği belirtilmektedir. Bu kapsamda, "owl:sameAs" ifadesinin hatalı kullanımlarının anomali olarak tespitine yönelik bir yaklaşım ortaya konulmaktadır. Hatalı konfigürasyon

tespitine yönelik bir başka ontoloji çalışması Cordova vd. [20] tarafından sunulmaktadır. İlgili çalışmada, güvenlik duvarı (*firewall*) sistemlerindeki yanlış konfigürasyonların anomali olarak tespit edilmesine yönelik ontoloji tabanlı bir sistem oluşturulmaktadır. Çalışmada, büyük işletmelerin, her biri kendi kural sözdizimine sahip farklı satıcılardan gelen çeşitli güvenlik duvarları kullandığı, güvenlik duvarlarında elle yapılandırılan kuralların yanlışlıklar içerebileceği ve bu yanlışlıkların tespitinin önemli olduğu vurgulanmaktadır. Bu kapsamda, güvenlik duvarı politikalarının doğrulanmasında gerekli hesaplama kaynaklarını azaltmaya yönelik bir ontoloji tasarımı sunulmaktadır.

Ontoloji tabanlı anomali tespit yaklaşımları, iş süreci yönetim sistemleri (*business process management system* – BPMS) gibi disiplinleri de uygulama alanı olarak kullanabilmektedir. Bu kapsamda, Sarno ve Sinaga'nın sunduğu çalışmada [21], süreç modellemeleri ve iş süreci yönetim sistemlerindeki süreçlere ait anomalilerin tespitine yönelik ontolojik bir model önerilmektedir. Çalışmada, birçok şirketin iş süreci yönetim sistemlerini kullanmakta olduğu, iş süreçlerindeki anomalilerin tespitinin şirketlere zarar verebilecek dolandırıcılık faaliyetlerine neden olabildiği belirtilmektedir. Bu kapsamda, iş süreç anomalilerinin tespitine yönelik ontoloji temelli süreç modellemesi ve birlik kuralı öğrenme (*association rule learning*) yöntemlerine dayalı Çok Seviyeli Sınıf Birlik Kuralı Öğrenme (*Multi-Level Class Association Rule Learning* - ML-CARL) isimli ontolojik bir model sunulmaktadır. Çalışmada, ortaya konulan modelin süreç anomalilerinin tespitinde %99'luk bir başarı sağladığı belirtilmektedir.

Anlamsal Web tabanlı anomali tespit çalışmalarında, metin içeriklerindeki anomalilerin de çalışma alanı olarak kullandığı görülmektedir. Ben-Abdallah vd. çalışmasında [22], sosyal medya yorumlarındaki istenmeyen içeriklerin anomali olarak tespitine yönelik olasılıklı ontolojiye dayalı bir yaklaşım sunulmaktadır. Çalışmada, sosyal medya platformlarındaki kullanıcı sayısının, gönderilere yapılan yorum sayısını doğru oranda etkilediği ve yorumlardaki zararlı içeriklerin anomali olarak tespitinin kritik olduğu belirtilmektedir. Bu kapsamda, olasılıklı web ontolojisi dili (*probabilistic web ontology language* – PR-OWL) kullanılarak bir zararlı içerik tespit ontolojisi (*review spam probabilistic ontology* – RSPO) yaratılmaktadır. Çalışmada, sunulan ontolojik yaklaşımın zararlı içerik tespitinde etkin sonuçlar ürettiği belirtilmektedir. Metin içeriklerindeki anomalilerin tespitine yönelik bir başka ontoloji çalışması Maurya vd. [23] tarafından sunulmaktadır. İlgili çalışmada, metin akışlarındaki beklenmedik yerel kalıpları tespit edebilecek Anlamsal Tarama (*Semantic Scan*, SS) adlı bir model önerilmektedir. Önerilen model, metin akışlarında beklenmedik anahtar kelime kalıplarıyla ortaya çıkan olayları tanımlamak için konu modellemesini (*topic modeling*) kullanmaktadır.

Anlamsal Web teknolojilerinin ve ontolojilerin karar destek sistemleri tarafından da sıklıkla kullanıldığı çalışmalar literatürde yer almaktadır. Riga vd. [24] tarafından sunulan çalışmada ontoloji tabanlı bir karar destek çerçevesi önerilmektedir. Bu kapsamda, karar alma sürecinin tüm aşamalarını eşit biçimde kapsayan bir çerçeve oluşturmak için ontolojilerden yararlanılarak verilerin yapılandırılması ve yeni bilgilerin çıkarılması sağlanmaktadır. Ishizu vd. [25], yönetim sistem denetiminde (*management system audit*) ontoloji tabanlı karar destek sistemleri için bir metodoloji sunmaktır. Rospocher ve Serafini [26] ise isteklerin yanıtlanmasında karar destek sistemi tarafından işlenen ve üretilen tüm içeriği ontolojik olarak temsil eden bir model önermektedir. Sağlık bilgi sistemlerinde karar destek sistemlerinin iyileştirilmesi ve esnekliğin arttırılmasını sağlamak için Anlamsal Web teknolojilerini temel alan bir yöntem Galopin vd. [27] tarafından önerilmektedir. Sherimon ve Krishnan [28] tarafından sunulan OntoDiabetic çalışmasında, risk faktörlerini değerlendirmek ve diyabetik hastalar için uygun tedavi önerileri sunmak için ontoloji tabanlı bir karar destek sistemi geliştirilmiştir. Alkahtani vd. [29], araba üretim alan bilgisini kullanarak ontoloji ve veri madenciliğine dayalı bir karar destek sistemi önermektedir. Böylelikle, arızalı parametrelerle ilgili üretim işlemleri ve önerilen değişikliklerin uygulanabilirliğini incelemek için onarım merkezindeki maliyet verileri tanımlanabilmektedir.

Sonuç olarak, ontoloji tabanlı anomali tespit yaklaşımlarının, bilgisayar ağları, web servisleri, akıllı ev sistemleri, süreç yönetim sistemleri, metin içerikleri ve işletim sistemleri gibi güvenlik düzeyi yüksek yapılardaki anormal durumların takibinde kullanıldığı görülmektedir. Bu çalışmada, dosya entegrasyonları kapsamında ağ ve işletim sistemlerindekine benzer olarak, entegrasyon sistemlerindeki anomalileri taramak için ontolojik bir model oluşturulması hedeflenmektedir. Bu kapsamda, bilgi güvenliğinin sağlanması temel alınarak veri bütünlüğü odaklı, anormal transferlerin tespitine yönelik bir anlamsal model yaratılmaktadır. Bu amaçla, dosya entegrasyonlarında anlamsal olarak ifade edilebilirlik sağlamaya yönelik bir bilgi tabanı oluşturulmaktadır. İlgili çalışmanın literatürdeki benzer çalışmalardan en temel farkı ve avantajı ise mevcut çalışmalarda dosya entegrasyonları özelinde bir etki alanının daha önce kullanılmamış olmasıdır. Mevcut çalışmalar ağ istekleri üzerindeki anomalilere odaklanmaktadır. Bu çalışmada ise, dosya entegrasyonu etki alanına yönelik bir anomali tespiti gerçekleştirilmesi amaçlanmaktadır. Literatür araştırması sonucunda, dosya entegrasyon sistemleri için bir anomali tespit sistemi ile karşılaşılmamış olduğundan önerilen çalışma ilgili alanda özgün bir yaklaşım sunmaktadır.

4. MATERYAL VE YÖNTEM (MATERIALS AND METHODS)

Ontoloji, kavramlar ve kavramlar arası ilişkilerin tanımlanmasıyla bilginin ortak bir terminoloji kullanılarak modellenmesidir. En tipik ontoloji türü, bir taksonomi ve bir dizi çıkarsama kuralından oluşmaktadır [30]. Ontolojiler; alan bilgisinin tekrar kullanılabilmesini, analiz edilebilmesini ve alan bilgisini operasyonel bilgiden ayırabilmek için kullanıcılar ve etmenler arasında ortak bir

kavram paylaşımı sunmaktadır [31]. Önerilen bu çalışma kapsamında da ontoloji temelli bir yapının oluşturulmasının amacı, dosya entegrasyonları alanı bazında yeniden kullanılabilir, genellenebilir ve operasyon bağımsız bir bilgi tabanı yaratmaktır. Dosya entegrasyonu ontolojsinin geliştiriminde Noy ve McGuiness'in [31] temel ontoloji geliştirme adımları kullanılmıştır.

4.1. Etki Alanını ve Ontoloji Kapsamını Belirleme (Determine the domain and scope of the ontology)

Ontoloji geliştirmede ilk adım olarak, geliştirilecek ontolojinin etki alanı ve kapsamı belirlenmelidir [31]. Dosya entegrasyonları ontolojisinin etki alanını ve kapsamını belirleme aşamasında da; ontolojinin etki alanının tanımı, ontolojinin hangi amaçla kullanılacağı, kimler tarafından kullanılacağı ve bakımını kimlerin yapacağı gibi temel sorulara yanıtlar aranmıştır. Bu sorular, ontoloji tasarımında modelin kapsamını sınırlamada önemli olmaktadır. Bu amaçla oluşturulan sorular ve cevapları aşağıdaki gibidir:

- *Geliştirilen ontoloji hangi etki alanını kapsamaktadır?*: Ontolojinin etki alanı dosya entegrasyonları işlemlerinde anomali tespiti olacaktır.
- *Geliştirilen ontoloji hangi amaçla kullanılacaktır?*: Bu ontoloji, dosya entegrasyonu temelli çalışan sistemlerde anormal durumların tespitini sağlamada kullanılacaktır. Dosya entegrasyonu ontolojisinin getireceği yenilik, mevcuttaki teknoloji ve operasyon bazlı anomali tespit sistemlerini genelleştirmek, yeniden kullanılabilir, etki alanı temelli bir yapı sağlamak ve bu alanda bir bilgi tabanı oluşturmak olacaktır.
- *Ontolojinin kullanımı ve bakımı kimler tarafından yapılacaktır?*: Ontoloji, dosya entegrasyonu ile çalışan sistemler ve uygulamalar tarafından kullanılacaktır. Ontolojinin bakımı da benzer şekilde dosya entegrasyon sistemleri tarafından yapılacaktır.

Geliştirilecek ontolojinin kapsamını belirlemek amacıyla bir dizi olası yeterlik (*competency*) sorusu belirlenmiştir. Yeterlik soruları, veritabanı sorguları ile çözümlenmeyecek soruları da kapsamalı, ancak sadece birer taslak olmalı ve detay içermemelidir [31]. Bu yeterlik soruları, geliştirilecek olan dosya entegrasyonu ontolojisindeki bilgiler ile yanıtlanabilecek sorular olmalıdır.

Dosya entegrasyonları etki alanında anomali tespiti özelindeki yeterlik soruları, entegrasyonlar sırasında sıkça karşılaşılan anomali belirtilerine göre oluşturulmuştur. Bu belirtiler aşağıda listelenmektedir:

- **Aşırı büyük boyutlara sahip dosyalar:** Entegre edilen dosyaların boyutu beklenenden büyükse bu durum bir dosya boyutu anomalisidir.
- **İçeriği olmayan dosyalar:** Entegre edilen dosyalarda veri yoksa (içerik boşsa) bu durum bir dosya boyutu anomalisidir.
- **Uzun süren entegrasyonlar:** Entegrasyon işlem süresi beklenenden uzun ise bu durum bir işlem süresi anomalisidir.
- **Durdurulmuş entegrasyonlar:** Entegrasyon işlem süresi sıfır (0) milisaniye ise hiç başlamamış demektir. Bu durum bir işlem süresi anomalisidir.
- **Başarısız entegrasyonlar:** Entegrasyon sırasında derleme hatası ya da askıya alınma gibi durumlar ile karşılaşılırsa bu entegrasyon başarıyla sağlanmamıştır. Bu da anormal nitelikli bir durum olarak ele alınır.

Bu belirtiler göz önüne alınarak oluşturulan yeterlik soruları aşağıdaki gibidir:

- Dosya boyutu sıfır (0) megabayt olan dosya transferleri anormal midir?
- Statüsü başarısız olan her entegrasyon anormal olarak mı kabul edilmelidir?
- En çok hangi sunucu üzerinde dosya transferi gerçekleşmektedir?
- Kritik düzeydeki entegrasyonlarda anormal nitelikli dosya transferleri mevcut mudur?
- Fatura entegrasyonu mu yoksa personel yönetimi entegrasyonu mu daha çok anormal nitelikli transfer içermektedir?
- Hangi entegrasyonun ortalama dosya boyutu daha büyüktür?
- Hangi entegrasyon daha uzun ortalama işlem süresine sahiptir?
- Fatura entegrasyonlarında canlı tipteki sunuculardaki mı yoksa test tipindeki sunuculardaki mı daha fazla transfer gerçekleşmiştir?
- Canlı sunuculardaki kaçar adet dosya transferi gerçekleşmiştir?
- TCDD entegrasyonunda işlem süresi bir dakikayı aşan transferler anormal midir?
- En sık olarak hangi teknolojik platformda entegrasyon geliştirimi yapılmaktadır?
- En sık hangi iletişim modeli ile dosya transferleri yapılmaktadır?

4.2. Mevcut Benzer Ontoloji Araştırması (Existing Similar Ontology Research)

Ontoloji geliştiriminde benzer etki alanlarını içeren ontolojileri tekrar kullanmak ve kapsamlarını genişletmek, türetilebilirlik ve yeniden kullanılabilirlik açısından önemlidir. Özel bir etki alanı için bir ontoloji oluşturmanın birkaç yolu vardır. Örneğin, ilgili etki alanında bulunan eski bir ontoloji genişletilebilir. Ontoloji oluşturmanın bir diğer yolu ise ilgili etki alanındaki mevcut taksonomiyi kullanarak yeni bir ontoloji yaratmaktır [12]. Bu doğrultuda dosya entegrasyonları ve anomali tespiti bazında yeniden kullanılabilir mevcut ontolojilerin araştırması yapılmıştır. Araştırma sonucunda, kurumsal entegrasyonların modellemesinde kullanılan ve benzer olabilecek TOVE ontolojisine [32] ulaşılmıştır.

TOVE ontolojisi, kurumsal ve ticari iş akışlarının modellenmesinde kullanılan geniş kapsamlı, genel amaçlı ve yeniden kullanılabilir bir ontolojidir [32]. Entegrasyon

mimarisine ait olayları kapsayan statü, zaman ve aktivite terminolojilerini içermektedir. Ancak, kurumsallığı temel alan çok genel kapsamlı bir ontoloji olduğu için dosya entegrasyonlarında anomali tespiti ihtiyacına cevap verecek bir yapı olarak düşünülmemiştir.

Dosya entegrasyonları kapsamında yapılan araştırma ve inceleme sonucunda, önerilen bu çalışmanın amacını kapsayan bir ontoloji bulunamamıştır. Bu nedenle, dosya entegrasyonları taksonomisini temel alan ve anomali tespitini yönelik yeni bir ontoloji geliştirilmiştir.

4.3. Önemli Terimlerin Belirlenmesi (Enumarating Important Terms)

Ontoloji modellemesinde üçüncü adım olarak, yaratılacak ifadelerde kullanılacak önemli dosya entegrasyon terimleri ortaya çıkarılmıştır. Bu doğrultuda; terimler, terimlerin tipleri ve özellikleri belirlenmiştir. Örneğin; "FileTransfer", "Integration" ve "Server" gibi ifadeler dosya entegrasyon alanında birer terim olarak belirlenebilmektedir. "Integration" teriminin "InvoiceIntegration", "WaybillIntegration" ve "PersonnelIntegration" gibi değişik tipleri olabilmektedir. Entegrasyonun öneminin derecesini belirten "IntegrationImportance" teriminin; "Critical", "Normal" ve "LowRisked" tipleri olabilir. "Server" teriminin ise "ProductionServer", "TestServer" ve "DevelopmentServer" gibi üç ayrı tipi belirlenebilir. Ayrıca, "FileTransfer" teriminin "TransferNumber", "FileName" ya da "Duration" gibi özellikleri olabilir. Sonuç olarak, bu ve benzeri terimler ontoloji geliştiriminin ileriki aşamalarında sınıf ve özellik hiyerarşilerinin oluşturumunda kullanılacaktır. Belirtilen kapsam doğrultusunda, dosya entegrasyon ontolojisi ile ilgili önemli terimler Tablo 1'de listelenmektedir.

Tablo 1. Dosya entegrasyonu terimleri
(Terms of file integration)

Dosya Entegrasyon Terimleri	
Integration	InvoiceIntegration
PersonnelIntegration	WaybillIntegration
WorkType	Momentary
Periodical	IntegrationImportance
Critical	Normal
LowRisked	Platform
MicrosoftPlatform	JavaPlatform
IBMPlatform	CommunicationModel
SmtpCommunication	WcfCommunication
RfcCommunication	AuthorizedPerson
Server	IpAddress
DevelopmentServer	TestServer
ProductionServer	FileTransfer
NormalTransfer	AnomalousTransfer
FileName	FileSize
FileType	StartTime
FinishTime	Duration
TransferNumber	ReTransmission
TransferStatus	Succeed
Failure	SuccessRatioLimit

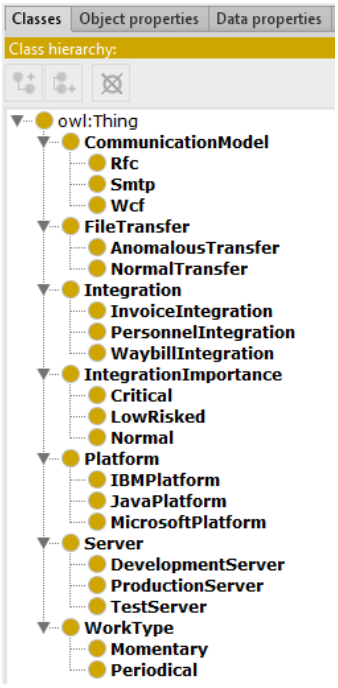
4.4. Sınıf Hiyerarşisi (The Class Hierarchy)

Dosya entegrasyonu ontolojisi kapsamında önemli terimler belirlendikten sonra bir sınıf hiyerarşisi oluşturulmuştur. Ontolojideki sınıflar ve sahip oldukları alt sınıflar aşağıda tanımlanmıştır:

- "Integration": Sistemdeki entegrasyonları temsil etmektedir. İki sistem arasındaki veri akış çeşidi olarak tanımlanmaktadır. Devletten özel şirketlere akan elektronik faturalar bu sınıfa bir örnektir. "InvoiceIntegration", "PersonnelIntegration" ve "WaybillIntegration" alt sınıflarına sahiptir.
- "Server": Sistemdeki sunucuları temsil etmektedir. Dosya transferleri sunucular üzerinde gerçekleşmektedir ve sunucular, iki sistem arasındaki dosyaların çevrimiçi olarak akmasını sağlamaktadır. "Server sınıfı, "TestServer", "ProductionServer" ve "DevelopmentServer" alt sınıflarına sahiptir.
- "FileTransfer": Sisteme entegrasyon bazında gelen dosya transferlerini temsil etmektedir. Her entegrasyon sınıfının dosya transferleri vardır. Ontolojinin amacı olan anormallik tespitinde kullanılacak ana sınıftır. "AnomalousTransfer" ve "NormalTransfer" olmak üzere iki alt sınıfa sahiptir.
- "Platform": Entegrasyonların gerçekleştiği teknoloji özelindeki platformları temsil etmektedir. Entegrasyon teknolojisi olarak da tanımlanabilir. "MicrosoftPlatform", "JavaPlatform" ve "IBMPlatform" alt sınıflarına sahiptir.
- "IntegrationImportance": Entegrasyonun önem kriterini belirten sınıftır. Bir sistemde entegrasyonlar değişik önem gruplarında olabilir. Organizasyonlarda kritik entegrasyonlara daha çok öncelik verilmektedir. "Critical", "Normal" ve "LowRisked" olmak üzere üç alt sınıfa sahiptir.
- "WorkType": Entegrasyonun anlık ya da periyodik çalışma tipini temsil eder. Sistemlerde periyodik olarak tetiklenen entegrasyonlar olacağı gibi, gönderici sistem bir dosya attığı anda tetiklenen entegrasyonlar da olabilmektedir. "Worktype" sınıfı, "Momentary" ve "Critical" alt sınıflarına sahiptir.
- "CommunicationModel": Entegrasyonun ağ iletişim modelini temsil eymektedir. Dosya entegrasyonları iletişim altyapısı için değişik teknolojiler kullanabilmektedir. Bu teknolojileri temsil eden "CommunicationModel" sınıfı, "RfcCommunication", "WcfCommunication" ve "SmtpCommunication" gibi alt sınıflara sahiptir.

Ontoloji sınıf hiyerarşisinin geliştiriminde Protégé ontoloji geliştirme ortamı [33] kullanılmıştır. Protégé, akıllı sistemler oluşturmak için kullanılan ücretsiz, açık kaynaklı bir ontoloji editörüdür. Geliştirilen sınıf hiyerarşisi Şekil 1'de görülmektedir.

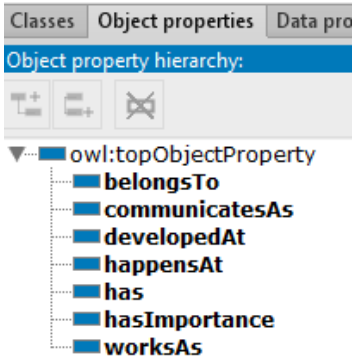
Şekil 1'de yer alan sınıf hiyerarşisi temel alınarak, dosya entegrasyonu ontolojisi kapsamında obje ve veri özellikleri çıkarılmış, sonrasında ise kısıtlar belirlenmiştir.



Şekil 1. Ontoloji sınıf hiyerarşisi
(The class hierarchy of the ontology)

4.5. Özellik Hiyerarşisi (The Property Hierarchy)

Ontoloji kapsamında belirlenen sınıfların aralarındaki ilişkileri temsil etmek amacı nesne özellik (*object property*) hiyerarşisi oluşturulmuştur. Özellik hiyerarşisinin Protégé ortamındaki gösterimi Şekil 2'de yer almaktadır.



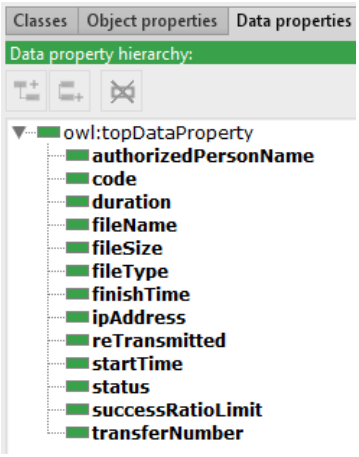
Şekil 2. Ontoloji nesne özellik hiyerarşisi
(The object property hierarchy of the ontology)

Ontoloji kapsamında yaratılan özelliklerin etki alanı-sınır (*domain-range*) değerleri oluşturulmuştur. Temel özellikler ve etki alanı-sınır bilgileri Tablo 2'de verilmektedir.

Tablo 2. Nesne özelliklerinin etki alanı-sınır bilgisi
(The domain-range information of object properties)

Özellik	Etki Alanı	Sınır
happensAt	FileTransfer	Server
belongsTo	FileTransfer	Integration
developedAt	Integration	Platform
communicatesAs	Integration	CommunicationModel
hasImportance	Integration	IntegrationImportance
worksAs	Integration	WorkType
has	Integration	FileTransfer

Nesne özellikleri sınıflar arasındaki ilişkileri tanımlarken, veri özellikleri (*data properties*) nesnelerin sahip olduğu özellikleri temsil etmektedir. Geliştirilen ontoloji özelinde yaratılan veri özelliklerinin Protégé ortamındaki gösterimi Şekil 3'de yer almaktadır.



Şekil 3. Ontoloji veri özellik hiyerarşisi
(The data property hierarchy of the ontology)

Şekil 3'te yer alan veri özelliklerinden "code", "successRatioLimit" ve "authorizedPersonName", "Integration" sınıfının veri özellikleridir. "FileTransfer" sınıfı; "fileName", "filesize", "transferNumber", "startTime", "finishTime", "duration", "fileType", "reTransmitted" ve "status" özelliklerini kullanmaktadır. "ipAddress" veri özelliği ise "Server" sınıfı tarafından kullanılmaktadır.

4.6. Özelliklerin Kısıtlamaları (Facets of Properties)

Dosya entegrasyonu ontolojisinde çıkarılan özellikler için bazı kısıtlamalar bulunmaktadır. Bu kısıtlamalar; veri tipi, izin verilen değerler ve kardinalite kısıtları bazında incelenmiştir. Ontolojide oluşturulan özelliklerin değer kısıtlamaları Tablo 3'te gösterilmektedir. Tabloda, ontoloji kapsamında yaratılan veri özelliklerinin temel olarak tekil kardinaliteye sahip olduğu görülmektedir. Böylelikle, bir sınıf ilgili özellikten yalnızca bir tane içerecektir. Yalnızca "authorizedPersonName" özelliği çoklu olup, bir entegrasyonun birden fazla sorumlusunun olabileceğini göstermektedir. Özelliklerin hepsi belirli veri tiplerine sahiptir. Bazı sayı (*number*) tipindeki özellikler için değer aralığı kısıtı belirlenmiş olup, "fileType" ve "status" gibi string tipindeki özellikler için ise enümere edilmiş string değer kümeleri, veri kısıtları olarak gösterilmiştir.

Dosya entegrasyon ontolojisinin sınıf hiyerarşisi, özellik hiyerarşisi ve özellik kısıtlamalarını gösteren diyagram Şekil 4 üzerinden görülebilmektedir.

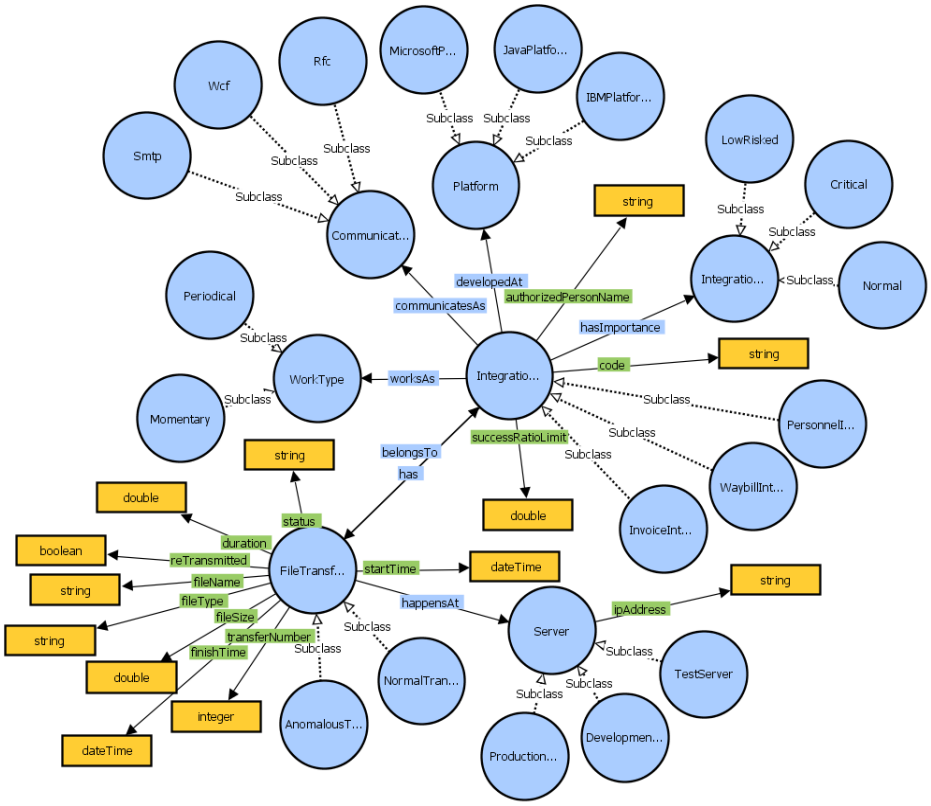
Şekil 4'teki diyagramda, dosya entegrasyon ontolojisini oluşturan temel sınıflar, bu sınıflara bağlı alt sınıflar, özellik hiyerarşisi, sınıfların temel özellikleri ve veri kısıtları görülmektedir. Ayrıca, Tablo 2'de ilk başta görülemeyecek olan ve "belongsTo" ile "has" özelliklerinin birbirinin ters özelliği (*inverse property*) olduğu da Şekil 4 üzerinden çıkarsanabilmektedir. Ontoloji geliştiriminin bir sonraki adımında da bu yapı üzerinden dosya entegrasyon etki alanında yeni varlıklar yaratılarak bir popülasyon oluşturulacaktır.

Tablo 3. Özellik kısıtlamaları (Property facets)

Özellik İsmi	Veri Tipi	Değer Aralığı	Kardinalite
status	xsd:string	"succeed" ya da "failed"	single
ipAddress	xsd:string	-	single
reTransmitted	xsd:boolean	0 ya da 1	single
fileType	xsd:string	"xml", "edi" ya da "excel"	single
duration	xsd:double	0'dan büyük	single
StartTime	xsd:dateTime	-	single
finishTime	xsd:dateTime	-	single
fileName	xsd:string	-	single
fileSize	xsd:double	0'dan büyük	single
transferNumber	xsd:integer	0'dan büyük	single
authorizedPersonName	xsd:string	-	multiple
successRatioLimit	xsd:double	0 ve 100 arası	single
code	xsd:string	-	single

4.7. Örnek Populasyon (Instance Population)

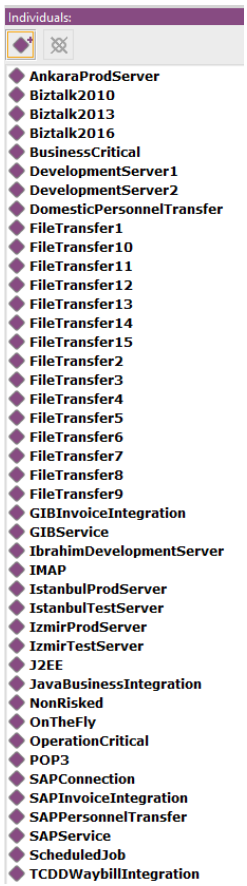
Dosya entegrasyon ontolojisi geliştiriminde yedinci adım olarak varlık yaratımı ve popülasyon oluşturma aşaması gerçekleştirilmiştir. Yaratılan ontoloji modeli için örnek varlıklar oluşturulmuştur. Örnek oluşturmada; (i) bir sınıf seçilmiş, (ii) o sınıftan bir birey yaratılmış ve (iii) o bireyin slot değerleri girilmiştir [13]. Ontolojideki her bir sınıf için Protégé ortamında örnekler oluşturulmuştur. Bu doğrultuda, alt sınıflar bazında oluşturulan örnek varlıklar Tablo 4'de verilmektedir. Yaratılan örneklerin Protégé ortamı üzerinden gösterimi Şekil 5'de görülmektedir.



Şekil 4. Ontoloji diyagramı
(The diagram of the ontology)

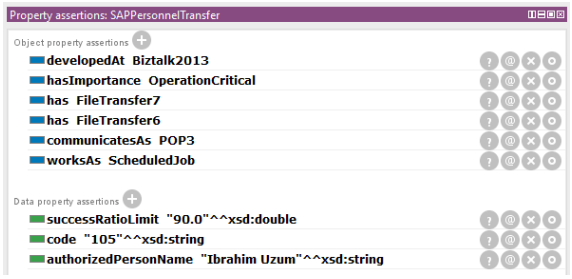
Tablo 4. Örnek varlıklar (Instances)

Sınıf Adı	Varlık ismi	Sınıf Adı	Varlık ismi
Rfc	SAPConnection	ProductionServer	IzmirProdServer
Rfc	YapiKrediRfc	Critical	BusinessCritical
Smtp	IMAP	Critical	OperationCritical
Smtp	POP3	InvoiceIntegration	GIBInvoiceIntegration
Wcf	GIBService	InvoiceIntegration	SAPInvoiceIntegration
Wcf	SAPService	WaybillIntegration	TCDDWaybillIntegration
Wcf	TCMBService	WaybillIntegration	TofasIntegration
Momentary	OnTheFly	PersonnelIntegration	DomesticPersonnelTransfer
Periodical	ScheduledJob	PersonnelIntegration	SAPPersonnelTransfer
IBMPlatform	WebSphere	FileTransfer	FileTransfer1
JavaPlatform	J2EE	FileTransfer	FileTransfer2
JavaPlatform	JavaBusinessIntegration	FileTransfer	FileTransfer3
MicrosoftPlatform	Biztalk2010	FileTransfer	FileTransfer4
MicrosoftPlatform	Biztalk2013	FileTransfer	FileTransfer5
DevelopmentServer	DevelopmentServer1	FileTransfer	FileTransfer6
DevelopmentServer	DevelopmentServer2	FileTransfer	FileTransfer7
TestServer	IstanbulTestServer	FileTransfer	FileTransfer8
TestServer	IzmirTestServer	FileTransfer	FileTransfer9
ProductionServer	IstanbulProdServer	FileTransfer	FileTransfer10

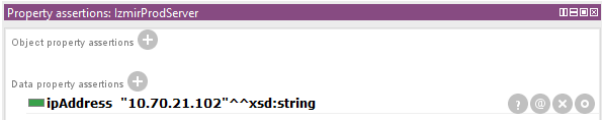


Şekil 5. Ontolojinin örnek varlıkları
(Instances of the ontology)

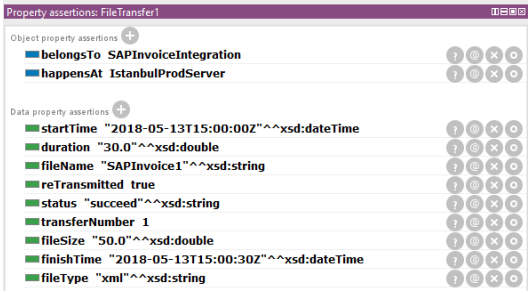
Varlık listesindeki her bir varlık için veri özelliği kapsamında slot değerleri girilmiştir. Ayrıca, nesne özelliği bulunan varlıkların da ilgili değerleri verilerek ilişkisel bir popülasyon yaratılmıştır. "Integration", "Server" ve "FileTransfer" sınıflarından türetilen alt sınıflara ait varlıklar örnek verilirse; nesne ve veri özellik savları (*object and data property assertions*) ve tanım (*description*) bilgilerinin Protégé ortamında temsili Şekil 6, 7 ve 8'de görümektedir.



Şekil 6. "SAPPersonalTransfer" örnek varlığı
("SAPPersonalTransfer" instance)

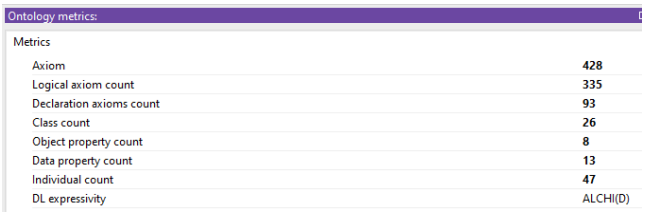


Şekil 7. "IzmirProdServer" örnek varlığı
("IzmirProdServer" instance)



Şekil 8. "FileTransfer1" örnek varlığı
("FileTransfer1" instance)

Şekil 6, 7 ve 8'de "PersonnelIntegration", "ProductionServer" ve "FileTransfer" sınıflarından sırasıyla türetilen "SAPPersonnelTransfer", "IzmirProdServer" ve "FileTransfer1" varlık örnekleri gösterilmektedir. Burada; varlık tanımlarının yanında varlıklara ait tip bilgisinin, ilişkisel özellik tanımlamalarının ve veri slot değerlerinin de tanımlandığı görülmektedir. İlgili tanımlar, ontoloji popülasyonu kapsamında oluşturulan bütün varlıklar için gerçekleştirilmiştir. Geliştirilen ontolojinin ontoloji metrikleri Şekil 9'da yer almaktadır.


Ontology metrics:

Metrics	
Axiom	428
Logical axiom count	335
Declaration axioms count	93
Class count	26
Object property count	8
Data property count	13
Individual count	47
DL expressivity	ALCHI(D)

Şekil 9. Ontoloji metrikleri (Ontology metrics)

4.8. Sorgular (Queries)

Ontoloji geliştirim kapsamında, Noy ve McGuiness'in [31] belirtmiş olduğu yedi temel adım tamamlanmıştır. Son aşama olarak, yaratılan ontoloji modelinde anormal dosya transferlerinin tespiti bazında çeşitli kurallar belirlenerek, bu kurallar üzerinden anormal bulgular elde edilmeye çalışılmıştır. Sorguların oluşturulmasında SPARQL sorgu dili [34] kullanılmıştır. SPARQL, RDF'te tutulan verileri çekmek ve manipüle etmek için kullanılan bir anlamsal sorgu dilidir. SPARQL dili; toplama, alt sorgular, olumsuzlama, ifadelerle değer oluşturma, genişletilebilir değer sınaması, kural oluşturma ve sorguları kısıtlama gibi özellikleri desteklemektedir. Ontolojiye ait SPARQL tabanlı sorgular oluşturulurken aşağıda verilen ön ekler tanımlanmıştır. Dosya entegrasyonu ontolojisine özel olarak "ent" ön eki kullanılmıştır.

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX ent: <http://www.semanticweb.org/ibrahim/
ontologies/2018/4/untitled-ontology-4#>
```

Dosya entegrasyonu etki alanı kapsamında anormal transferlerin tespitini sağlamak için çeşitli kurallar tanımlanmıştır. Bu kuralların oluşturulmasında, genel iş gereksinimlerinin yanında entegrasyonlar özelindeki normlar da dikkate alınmıştır. Kurallar bütün dosya transferlerini ilgilendirmesinin yanında, entegrasyon, sunucu ya da kritiklik gibi özel durumlara da indirgenebilmektedir. Bunun anlamı, kuralların iş gereksinimleri doğrultusunda özelleştirilebilir olacağıdır. Dosya entegrasyonu ontolojisi bazında oluşturulan örnek kurallar temel olarak aşağıdaki gibidir:

- Tüm entegrasyonlarda, işlem süresi 0 (sıfır) saniye olan dosya transferleri anormaldir.
- Tüm entegrasyonlarda, dosya boyutu 0 (sıfır) byte olan dosya transferleri anormaldir.
- Kritik düzeydeki entegrasyonlarda bir dakika üzeri süren dosya transferleri anormaldir.
- Düşük riskli entegrasyonlarda iki dakika üzeri süren dosya transferleri anormaldir.
- Canlı sunuculara 100 MB dosya boyutunu aşan dosya transferleri anormaldir.
- Test sunuculara 200 MB dosya boyutunu aşan dosya transferleri anormaldir.
- GIB Fatura Entegrasyonu'na ait dosya transferlerinde 100 MB üzeri dosya boyutları ya da bir dakika üzeri işlem süreleri anormaldir.
- TOFAŞ Entegrasyonu'na ait dosya transferlerinde 150 MB ve 180 MB arasında olmayan dosya boyutları anormaldir.

Ontoloji kapsamında deneysel olarak oluşturulan SPARQL CONSTRUCT tanımları aşağıda verilmektedir:

- *Tüm entegrasyonlarda, işlem süresi 0 (sıfır) saniye olan dosya transferleri anormaldir.*

```
CONSTRUCT { ?transfer a ent:AnomalousTransfer }
WHERE { ?transfer rdf:type ent:FileTransfer .
        ?transfer ent:duration ?duration  .
        FILTER(?duration = 0) }
```

- *Tüm entegrasyonlarda, dosya boyutu 0 (sıfır) byte olan dosya transferleri anormaldir.*

```
CONSTRUCT { ?transfer a ent:AnomalousTransfer }
WHERE { ?transfer rdf:type ent:FileTransfer .
        ?transfer ent:fileSize ?fileSize  .
        FILTER (?fileSize = 0) }
```

- *Kritik düzeydeki entegrasyonlarda bir dakika üzeri işlem zamanına sahip dosya transferleri anormaldir.*

```
CONSTRUCT { ?transfer a ent:AnomalousTransfer }
WHERE { ?transfer rdf:type ent:FileTransfer .
        ?transfer ent:belongsTo ?integration .      ?integration
ent:hasImportance
    ent:BusinessCritical .
        ?transfer ent:duration ?duration  .
        FILTER (?duration > 60) }
```

- *Düşük riskli entegrasyonlarda iki dakika üzeri işlem zamanına sahip dosya transferleri anormaldir.*

```
CONSTRUCT { ?transfer a ent:AnomalousTransfer }
WHERE { ?transfer rdf:type ent:FileTransfer .
        ?transfer ent:belongsTo ?integration .      ?integration
ent:hasImportance
         ent:LowRisked.
        ?transfer ent:duration ?duration  .
        FILTER (?duration > 120) }
```

- *Canlı (production) sunucularda dosya boyutu 100 MB'ı aşan dosya transferleri anormaldir.*

```
CONSTRUCT { ?transfer a ent:AnomalousTransfer }
WHERE { ?transfer rdf:type ent:FileTransfer .
        ?transfer ent:happensAt
         ent:ProductionServer .
        ?transfer ent:fileSize ?fileSize  .
        FILTER (?fileSize > 100) }
```

- *Test sunucularında dosya boyutu 250 MB'ı aşan dosya transferleri anormaldir.*

```
CONSTRUCT { ?transfer a ent:AnomalousTransfer }
WHERE { ?transfer rdf:type ent:FileTransfer .
        ?transfer ent:happensAt ent:TestServer .
        ?transfer ent:fileSize ?fileSize  .
        FILTER (?fileSize > 50) }
```

- *GIB Fatura Entegrasyonu'na ait dosya transferlerinde 100 MB üzeri dosya boyutları ya da bir dakika üzeri işlem süreleri anormaldir.*

```
CONSTRUCT { ?transfer a ent:AnomalousTransfer }
WHERE { ?transfer rdf:type ent:FileTransfer .
        ?transfer ent:belongsTo
         ent:GIBInvoiceIntegration .
        ?transfer ent:fileSize ?fileSize  .
        ?transfer ent:duration ?duration  .
  FILTER (?fileSize > 100 || ?duration > 60) }
```

- *TOFAŞ Entegrasyonu'na ait dosya transferlerinde 150 MB ve 180 MB arasında olmayan dosya boyutları anormaldir.*

```
CONSTRUCT { ?transfer a ent:AnomalousTransfer }
WHERE { ?transfer rdf:type ent:FileTransfer .
        ?transfer ent:belongsTo
          ent:TofasIntegration .
        ?transfer ent:fileSize ?fileSize  .
 FILTER (?fileSize > 180 || ?fileSize < 150) }
```

Belirtilen bu kurallar, dosya entegrasyon ontolojisine ait örnek popülasyondaki anormal transferlerin tespitini sağlamaktadır. Yukarıda belirtilen "*Kritik düzeydeki entegrasyonlarda bir dakika üzeri işlem zamanına sahip dosya transferleri anormaldir.*" kuralının çalıştırılması sonucu elde edilen sorgu sonucu Şekil 10'da yer almaktadır.

SPARQL query:

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX ent: <http://www.semanticweb.org/ibrahim/ontologies/2018/4/untitled-ontology-4#>
CONSTRUCT { ?transfer a ent:AnomalousTransfer }
          WHERE {  ?transfer rdf:type ent:FileTransfer .
                   ?transfer ent:belongsTo ?integration .
                   ?integration ent:hasImportance ent:BusinessCritical .
                   ?transfer ent:duration ?duration  .
             FILTER (?duration > 60) }
```

Subject	Predicate	Object
FileTransfer3	rdf:type	AnomalousTransfer

Şekil 10. SPARQL sorgu örneği-1
(SPARQL query example-1)

SPARQL query:

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX ent: <http://www.semanticweb.org/ibrahim/ontologies/2018/4/untitled-ontology-4#>
CONSTRUCT { ?transfer a ent:AnomalousTransfer }
          WHERE {  ?transfer rdf:type ent:FileTransfer .
                   ?transfer ent:belongsTo ent:GIBInvoiceIntegration .
                   ?transfer ent:fileSize ?fileSize  .
                   ?transfer ent:duration ?duration  .
             FILTER (?fileSize > 100 || ?duration > 60) }
```

Subject	Predicate	Object
FileTransfer5	rdf:type	AnomalousTransfer

Şekil 11. SPARQL sorgu örneği-2
(SPARQL query example-2)

Şekil 11'de GIB Fatura entegrasyonu için belirlenen "*GIB Fatura Entegrasyonu'na ait dosya transferlerinde 100 megabayt üzeri dosya boyutları ya da bir dakika üzeri işlem süreleri anormaldir.*" sorgusunun sonuçları gösterilmektedir. Kritik düzeydeki entegrasyonlar özelinde yapılan kural tanımına göre, "FileTransfer3" varlığı anormal bir dosya transferidir. Benzer şekilde, "FileTransfer5" varlığı da GIB Fatura entegrasyonu kuralı özelinde anormal niteliklidir. Ontoloji kapsamındaki bu kurallar, popülasyondaki diğer entegrasyonlar özelinde de genişletilebilir.

Ontoloji geliştirimi kapsamında ek olarak, birinci adımda belirlenmiş olan karşılaştırma sorularının bir kısmı SPARQL sorguları ile işletilmiştir. Bu sorgular, dosya entegrasyonu ontolojisindeki bilgiler kullanılarak

yanıtlanabilir durumdadır. Oluşturulan SPARQL sorguları ve sözel tanımları aşağıdaki gibidir:

- *En çok hangi sunucu üzerinde dosya transferi gerçekleşmektedir?*

```
SELECT ?server
(COUNT(?transfer) AS ?transfercount)
WHERE { ?transfer rdf:type ent:FileTransfer .
        ?transfer ent:happensAt ?server  . }
GROUP BY ?server
ORDER BY DESC (?transfercount) LIMIT 1
```

- *TCDD entegrasyonunda işlem süresi bir dakikayı aşan transferler anormal midir?*

```
SELECT ?integration
(COUNT(?transfer) AS ?transferCount)
WHERE { ?transfer rdf:type ent:FileTransfer .
        ?transfer ent:belongsTo ?integration  .
        ?transfer rdf:type ent:AnomalousTransfer .
        ?integration rdf:type
         ent:TCDDWaybillIntegration .
        ?transfer ent:duration ?duration  .
        FILTER (?duration > 60)}
GROUP BY ?integration
```

- *Hangi entegrasyonun ortalama dosya boyutu daha büyüktür?*

```
SELECT ?integration
(AVG(?fileSize) AS ?avgFileSize)
WHERE { ?transfer rdf:type ent:FileTransfer .
        ?transfer ent:belongsTo ?integration  .
        ?transfer ent:fileSize ?fileSize  . }
GROUP BY ?integration
ORDER BY DESC (?avgFileSize) LIMIT 1
```

- *Hangi entegrasyon daha uzun ortalama işlem süresine sahiptir?*

```
SELECT ?integration
(AVG(?duration) AS ?avgDuration)
WHERE { ?transfer rdf:type ent:FileTransfer .
        ?transfer ent:belongsTo ?integration  .
        ?transfer ent:duration ?duration  . }
GROUP BY ?integration
ORDER BY DESC (?avgDuration) LIMIT 1
```

- *Fatura entegrasyonu mu yoksa personel yönetimi entegrasyonu mu daha çok anormal nitelikli transfer içermektedir?*

```
SELECT ?integration
(COUNT(?transfer) AS ?transferCount)
WHERE { ?transfer rdf:type ent:FileTransfer .
        ?transfer ent:belongsTo ?integration  .
        ?transfer rdf:type ent:AnomalousTransfer .
        ?integration rdf:type ?integrationType .
        FILTER (?integrationType =
         ent:SAPInvoiceIntegration|| ?integrationType =
         ent:GIBInvoiceIntegration)}
GROUP BY ?integration
ORDER BY ?transferCount LIMIT 1
```

- Kritik düzeydeki entegrasyonlarda anormal nitelikli dosya transferleri mevcut mudur?

```
SELECT ?integration
(COUNT(?transfer) AS ?transfercount)
WHERE { ?transfer rdf:type ent:FileTransfer .
        ?integration ent:hasImportance
          ent:BusinessCritical .
        ?transfer ent:belongsTo ?integration  .
        ?transfer ent:duration ?duration  .
      FILTER (?duration > 120)}
GROUP BY ?integration
ORDER BY DESC (?transfercount)
```

Belirtilen bu sorgular, dosya entegrasyonu etki alanında genel amaçlı ve anomali tespiti özelinde karşılaştırma ve ontoloji yetkinliğini sınayacak şekilde seçilmiştir. Sorgular, genel kapsamlı olmalarının yanı sıra; entegrasyon, sunucu ve platform gibi sınıflar özelinde de olabilmektedir. Son olarak, karşılaştırma soruları ontoloji bazında oluşturulan popülasyonun üzerinde işletilmiştir.

5. DEĞERLENDİRME (DISCUSSION)

Bu çalışmada dosya entegrasyonlarında anomali tespitine yönelik anlamsal bir yaklaşım ortaya konulmuştur. Çalışmanın temel amacı, teknoloji ve platform bağımsız bir yapı yaratmak ve dosya entegrasyonları gibi güvenlik düzeyi yüksek etki alanlarındaki anomali tespitlerinde bir anlamsal ifade edilebilirlik sunmaktır.

İşletim sistemleri, saldırı tespit sistemleri, gerçek zamanlı veri akışları, metin içerikleri ve mobil iletişim gibi güvenlik düzeyi yüksek uygulama alanlarındaki anormal bulguların tespitini sağlayan çalışmalara yönelik yapılan araştırmalarda, makine öğrenimine bağlı veri kümelemesi ve sınıflandırması modellerinin kullanımının daha yaygın olduğu görülmektedir [35, 36]. Ancak elde edilen tecrübelere göre, kural tabanlı anlamsal modellemenin de bu tip çalışmalar için bir alternatif olup, makine öğrenimi tekniklerine karşı belirli avantajlara sahip olduğu sonucuna varılmaktadır. Çalışmalardan edinilen tecrübeye göre, Anlamsal Web'in bilginin daha derin, standart temelli, genişletilebilir, türetilebilir ve anlamlandırılmış biçimde temsiline izin verebildiği görülmektedir. Dosya entegrasyonu etki alanında genel bir ontolojinin yaratılabilmesi ve ontolojinin anomali tespiti bazlı sorulara yanıtlar verebilmesi, bu görüşün doğruluğunu desteklemektedir. Ontoloji geliştiriminde elde edilen sonuçlara göre, kural tabanlı anlamsal yaklaşımların anomali tespitlerinde uygulanabilir olduğu sonucuna varılmaktadır.

Ontoloji tabanlı anomali tespit çalışmalarında anlamsal temsilin belirli avantajlar sunmaktadır. Dosya entegrasyonu ontolojisi örnek alındığında, farklı teknoloji ya da platformlardaki entegrasyon sistemlerinde bu tür anomali tespitleri için çoğunlukla farklı altyapıları birbirine entegre etmek gerekecektir. Geliştirilen anlamsal model ile bu sorun çözülmekte ve teknoloji bağımsız bir anomali tespit yapısı ortaya konmaktadır. Ek olarak, güvenlik düzeyi kritik uygulama alanlarındaki anomali tespitlerinde genel olarak yaşanan sorunlardan biri yapısal verinin elde edilmesindeki maliyettir. Anlamsal Web tabanlı bir çözüm yaklaşımı, ontolojiler ile değişik teknolojilerdeki dosya entegrasyonlarına ait bilgilerin birbirine entegre olmasını gerektirmeyecek şekilde bir kurgu oluşturabilmektedir. Operasyon ve teknoloji

bağımsız olmak birinci amaç olduğundan, eldeki veri her zaman standart bir yapıda olacak ve bu maliyet minimuma indirgenecektir.

Literatürde ağırlıklı olarak yer alan anomali tespiti bazlı ontoloji çalışmaları genel olarak bilgisayar ağı sistemleri [12, 13, 14], işletim sistemleri [15] ve web uygulamalarını [16] etki alanı olarak kullanmaktadır. Önerilen bu çalışma, ontoloji çalışmalarına dosya entegrasyonlarını yeni bir etki alanı olarak sunmaktadır. Sonuç olarak, anomali tespitlerinde anlamsal ifade edilebilirliğin; anormal bulguların etiketlenmesi için standart bir veri yapısı sunması, teknoloji ve operasyon bağımsız olması, etki alanı özelini temsil ediyor olması ve kural tabanlı güvenilir bir etiketleme mekanizması sağlaması sebebiyle dosya entegrasyonları etki alanı için literatürde bir alternatif olacağı değerlendirilmektedir.

6. SONUÇ VE GELECEK ÇALIŞMALAR (CONCLUSION AND FUTURE WORKS)

Bilgi sistemleri için gerçek zamanlı dosya entegrasyonlarının önemi gün geçtikçe artmaktadır. Entegrasyon sistemleri gibi güvenlik düzeyi yüksek yapılarda anomali tespit mekanizmalarının bulunması oldukça kritiktir. Dosya entegrasyonu temelli çalışan sistemlere günlük ortalama yarım milyon adet dosya transferi sağlanabilmektedir. Bu transferlerdeki anomalilerin zamanında belirlenmesi; dosya içeriğinin kontrolü ve müdahalesini, bilgi güvenliği bakımından dosyadaki veri bütünlüğü kapsamındaki ihlallerin önüne geçilebilmesini ve anormalliklerin izlenebilirliğini sağlayacaktır. Anomali tespiti kapsamında ontoloji tabanlı bir yapı ortaya koymak, genişletilebilirlik ve yeniden kullanılabilirlik açısından önemlidir. Önerilen çalışmada, dosya entegrasyonlarında anomali tespiti için anlamsal bir ifade edilebilirlik ortaya koymak amaçlanmıştır. Ontoloji geliştirimi kapsamında ilk olarak, ontolojinin tanımı ile kapsadığı etki alanı belirlenmiş ve benzer ontolojiler araştırılmıştır. Sonrasında, dosya entegrasyonları taksonomisindeki önemli terimler ortaya çıkarılmıştır. Bu terimlerden yola çıkılarak bir sınıf hiyerarşisi oluşturulmuş, sınıf hiyerarşisi temel alınarak, bir özellik hiyerarşisi oluşturulmuş ve bu özelliklerin kısıtlamaları yaratılmıştır. Dosya entegrasyonu taksonomisindeki birtakım örnekler kullanılarak örnek varlıklar oluşturulmuş ve ontolojinin popülasyonu sağlanmıştır. Oluşturulan bu popülasyon üzerinden anomali tespiti bazında çeşitli kurallar tanımlanmış ve anormal transfer bulguları incelenmiştir. Son olarak, yetkinlik soruları kapsamında ontoloji popülasyonu üzerinde örnek sorgular oluşturulmuştur. Gelecek çalışmalar kapsamında, önerilen bu yaklaşımın Apache Jena çerçevesi [37] kullanılarak uygulanması hedeflenmektedir. Ek olarak, [7, 8] çalışmalarında önerilen makine öğrenmesi yaklaşımları kullanılarak anomali tespit sisteminin hızlı ve doğruluk yüzdesi yüksek bir sonuç vermesi hedeflenen ve kendi kendine öğrenen anomali tespit sistemi ile bu çalışmada önerilen ontoloji tabanlı yaklaşımın entegre edilmesine yönelik çalışmalar gerçekleştirilmesi hedeflenmektedir.

KAYNAKLAR (REFERENCES)

[1] V. Chandola, A. Banerjee, V. Kumar, “Anomaly Detection : A Survey”, *ACM Computing Surveys (CSUR)*, 41(3), Article No 15, 2009.

[2] A. H. Hamamoto, L. F. Carvalho, L. D. H. Sampaio, T. Abrão, M. L. Proença Jr., “Network Anomaly Detection System using Genetic Algorithm and Fuzzy Logic”, *Expert Systems with Applications*, 92(C), 390-402, 2018.

[3] M. Ahmeda, A. N. Mahmooda, Md. R. Islam, “A survey of anomaly detection techniques in financial domain”, *Future Generation Computer Systems*, 55(C), 278-288, 2016.

[4] M. Hauskrecht, M. Valko, B. Kveton, S. Visweswaran G. F. Cooper, “Evidence-based Anomaly Detection in Clinical Domains”, **AMIA Annual Symposium Proceedings/AMIA Symposium**, 319-323, 2017.

[5] Internet: W3C, Extensible Markup Language (XML), https://www.w3.org/XML/ , 23.11.2018.

[6] Internet: F. Arnaboldi, OWASP - XML Security Cheat Sheet, , https://www.owasp.org/index.php/XML_Security_Cheat_Sheet, 23.11.2018

[7] İ. Üzüm, Ö. Can, “An anomaly detection approach for enterprise file integration”, **6th International Symposium on Digital Forensic and Security (ISDFS 2018)**, Antalya, Turkey, March 22-25, 2018.

[8] İ. Üzüm, Ö. Can, “An anomaly detection system proposal to ensure information security for file integrations”, **26th Signal Processing and Communications Applications Conference (SIU 2018)**, Izmir, Turkey, 1-4, 2-5 May, 2018.

[9] Ö. Can, M. Ünalır, “Ontoloji Tabanlı Bilgi Sistemlerinde Politika Yönetimi”, *Bilişim Teknolojileri Dergisi*, 3(2), 1-16, 2010.

[10] Ö. Gümüş, Ö. Gürcan, O. Dikenelli, “Anlamsal Servis Aracılığı İçin Bir Çok Etmenli Sistem ve Aracılık Etkileşim Protokolü”, *Bilişim Teknolojileri Dergisi*, 5(2), 9-24, 2012.

[11] Ö. Öztürk, “Petrol, Gaz ve Madencilik Endüstrisinde Bilgi Gösterimi için Ontoloji Temelli bir Yaklaşım”, *Bilişim Teknolojileri Dergisi*, 12(2), 147-158, 2019.

[12] F. Abdoli, M. Kahani, “Ontology Based Distributed Intrusion Detection System”, **In 14th International CSI Computer Conference**, Tehran, Iran, 65-70, 20-21 Oct., 2009.

[13] C. Hsieh, R. Chen, Y. Huang, “Applying an Ontology to a Patrol Intrusion Detection System for Wireless Sensor Networks”, *International Journal of Distributed Sensor Networks*, 10(1), doi: 10.1155/2014/634748, 2014.

[14] S. Hung, D. S. Liu, “A user-oriented ontology-based approach for network intrusion detection”, *Computer Standards & Interfaces*, 78-88, 2008.

[15] O. Can, O., M. O. Unalir, E. Sezer, O. Bursa, B. Erdogdu, “An Ontology Based Approach For Host Intrusion Detection Systems”, **In: 11th International Conference on Metadata and Semantic Research (MTSR 2017)**, Garoufallou E., Virkus S., Siatri R., Koutsomiha D. (eds), Communications in Computer and Information Science, Springer, Cham, Tallinn, Estonia, 755, 80-86, November 28 – December 1, 2017.

[16] G. Kolaczek, K.Juszczyszyn, "Attack pattern analysis framework for multiagent intrusion detection system", *International Journal Of Computational Intelligence Systems*, 1(3), 215-224, 2008.

[17] H. A. Karande, S. S. Gupta, S., S., "Ontology based Intrusion Detection System for Web Application Security", **In: International Conference On Communication Networks (ICCN)**, IEEE, Gwalior, India, 228-232, 19-21 November, 2015.

[18] E. Pardo, D. Espes, P. Le-Parc, "A Framework for Anomaly Diagnosis in Smart Homes Based on Ontology", *Procedia Computer Science*, 83, 80-86, 2016.

[19] J. Raad, W. Beek, F. van Harmelen, N. Pernelle, F. Sais, "Detecting Erroneous Identity Links on the Web Using Network Metrics", **In: International Semantic Web Conference (ISWC)**, Springer, Cham, 11136, 391-407, 2018.

[20] R. F. Cordova, A. L. Marcovich, C. A. Santivanez, "An Efficient Method for Ontology-Based Multi-Vendor Firewall Misconfiguration Detection: A Real-Case Study", **In: IEEE ANDESCON**, IEEE, Santiago de Cali, Colombia, 1-3, 2018.

[21] R. Sarno, F. P. Sinaga, "Business process anomaly detection using ontology-based process modelling and Multi-Level Class Association Rule Learning", **In: International Conference on Computer, Control, Informatics and its Applications (IC3INA)**, IEEE, Bandung, 12-17, 2015.

[22] E. Ben-Abdallah, K. Boukadi, M. Hammami, "Spam Detection Approach for Cloud Service Reviews Based on Probabilistic Ontology", **In: OTM Confederated International Conferences "On the Move to Meaningful Internet Systems"**, Springer, Cham, 11229, 534-551, 2018.

[23] A. Maurya, K. Murray, Y. Liu, C. Dyer, W. W. Cohen, D. B. Neill, "Semantic Scan: Detecting Subtle, Spatially Localized Events in Text Streams", *Information Retrieval*, Cornell University, doi: 10.1145/1235, 2016.

[24] M. Riga, E. Kontopoulos, K. Karatzas, S. Vrochidis, I. Kompatsiaris, "An Ontology-Based Decision Support Framework for Personalized Quality of Life Recommendations", **In: Decision Support Systems VIII: Sustainable Data-Driven and Evidence-Based Decision Support (ICDSST 2018)**, Lecture Notes in Business Information Processing, 313, 38-51, 2018.

[25] S. Ishizu, A. Gehrmann, J. Minegishi, Y. Nagai, "Ontology-Driven Decision Support Systems For Management System Audit", **In: Proceedings of the 52nd Annual Meeting of the ISSS - 2008**, Madison, Wisconsin, 2008.

[26] M. Rospocher, L. Serafini L., "An Ontological Framework for Decision Support", **In: Joint International Semantic Technology Conference-Semantic Technology (JIST 2012)**, Lecture Notes in Computer Science, 7774, 239-254, 2013.

[27] A. Galopina, J. Bouaude, S. Pereira, B. Seroussi, "An Ontology-Based Clinical Decision Support System for the Management of Patientswith Multiple Chronic Disorders", *Stud Health Technol Inform.*, 216-275, 2015.

[28] P. C. Sherimon, R. Krishnan, *Arabian Journal for Science and Engineering*, 41(3), 1145–1160, 2016.

[29] M. Alkahtani, A. Choudhary, A. De, J. A. Harding, "A decision support system based on ontology and data mining to improve design using warranty data*", Computers & Industrial Engineering*, 128, 1027–1039, 2019.

[30] T. Berners-Lee, J. Hendler, O. Lassila, "The Semantic Web", *Scientific American*, 284(5), 28-37, 2001.

[31] Internet: N. F. Noy, D. L. McGuiness, Ontology Development 101: A Guide to Creating Your First Ontology, Stanford University, Stanford, CA, 25p., https://protege.stanford.edu/publications/ontology_ development/ontology101.pdf

[32] Internet: M. S. Fox, Enterprise Integration Laboratory, TOVE Ontologies, http://www.eil.utoronto.ca/theory/enterprise-modelling/ tove/, 23.11.2018

[33] Internet: Stanford University, Protégé Ontology Editor, https://protege.stanford.edu/, 23.11.2018

[34] Internet: World Wide Web Consortium, SPARQL Query Language for RDF, W3C Recommendation 15 January 2008, https://www.w3.org/TR/rdf-sparql-query/, 23.11.2018

[35] S. Agrawal, J. Agrawal, "A Survey on Anomaly Detection using Data Mining Techniques", **In: 19th International Conference on Knowledge Based and Intelligent Information and Engineering Systems** , Elsevier B. V., 60, 708-713, 2015.

[36] S. Ahmad, A. N. Mahmood, J. Hu, "A Survey of Network Anomaly Detection Techniques", *Journal of Network and Computer Applications*, 60, 19-31, 2015.

[37] Internet: Apache Jena, A free and open source Java framework for building Semantic Web and Linked Data applications, https://jena.apache.org, 23.11.2018.